Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-14. **(Cancelled)**

15. **(Previously Presented)** The method of claim 34, wherein said corresponding part of the first chain of operations corresponding to the at least a part of the second chain of operation comprises an exclusive OR.

16. **(Previously Presented)** The method of claim ~~14~~ 34, wherein said corresponding part of the first chain of operations corresponding to the at least a part of the second chain of operations comprises an operation of bit permutation of an intermediate result obtained by carrying out operations of said second chain of operations preceding this operation of bit permutation.

17. **(Previously Presented)** The method of claim 34, wherein said corresponding part of the first chain of operations corresponding to the at least a part of the second chain of operations comprises an operation of indexed access to a table.

18. **(Previously Presented)** The method of claim 34, wherein said corresponding part of the first chain of operations corresponding to the at least a part of the second chain of operations comprises an operation which is stable with respect to the application of an exclusive OR function.

19. **(Previously Presented)** The method of claim 18, wherein said corresponding part of the first chain of operations corresponding to the at least a part of the second chain of operations is an operation of transfer of an intermediate result obtained by carrying out operations of said second chain of operations preceding this operation of transfer, from one location to another one in a storage space.

20. **(Previously Presented)** The method of claim 34, wherein the step of randomly selecting comprises identifying a series of several parts within the first chain of operations and comprises randomly selecting, for each part of said series of several parts of the first chain of operations, said part in either a normal state or in a complemented state.

21. **(Previously Presented)** The method of claim 34, wherein the step of randomly selecting comprises identifying a series of several operations within the first chain of operations, and comprises randomly selecting, for each operation of said series of operations of the first chain of operations, such operation either in a normal state or in a complemented state.

22. **(Previously Presented)** The method of claim 20, wherein the step of randomly selecting is conducted depending on the state of a random parameter generated for each part of the series of several parts within this first chain of operations and comprises updating a complementation counter, and the step of selecting to output as the resultant message the result of the last operation in either in a same state or in a complemented state is decided depending on the state of the complementation counter.

23. **(Previously Presented)** The method of claim 20, wherein the step of randomly selecting is conducted depending on the state of a random parameter generated for each part of the series of several parts within this first chain of operations and comprises transmitting, for each part of said series of several parts within this first chain of operations, information to be used during the step of outputting as the resultant message the result of the last operation in a same state of in a complemented state.

24. **(Previously Presented)** The method of claim 20, wherein the step of randomly selecting comprises a step of computing a parameter which is equal to a difference between the number of times when an operation of the second chain of operations is in the same state as in the first chain of operations and the number of times when an operation of the second chain of operations of the chain is in complemented state, and when this difference exceeds a given threshold, the step of randomly selecting a next part of the series of several parts in a normal state or in a complemented state is conducted so as to decrease this difference.

25. - 26. **(Cancelled)**

27. **(Previously Presented)** The method of claim 34, wherein the complemented state of said corresponding part of the first chain of operations corresponding to the at least a part of the second chain of operations is obtained by a complementation carried out byte by byte.

28. **(Previously Presented)** The method of claim 34, wherein the complemented state of said corresponding part of the first chain of operations corresponding to the at least a part of the second chain of operations is obtained by a complementation carried out bit by bit.

29. **(Previously Presented)**The method of claim 34, wherein the step of having the microcircuit entity determine the second chain of operations further comprises a step of determining a permutation of the order of successive commutative operations in the first chain of operations.

30. **(Previously Presented)** The method of claim 29, wherein the step of determining a permutation of the order of successive commutative operations is carried out randomly.

31. **(Previously Presented)** The method of claim 21, wherein the step of randomly selecting is conducted depending on the state of a random parameter generated for each operation of the series of several operations within the first chain of operations and comprises updating a complementation counter, and the step of selecting to output as the resultant message the result of the last operation in either in a same state or in a complemented state is decided depending of the state of the complementation counter.

32. **(Previously Presented)** The method of claim 21, wherein the step of randomly selecting is conducted depending of the state of a random parameter generated for each operation of the series of several operations of the first chain of operations and

comprises transmitting, for each operation of the series of operations within the first chain of operations, information to be used during the step of outputting as the resultant message the result of the last operation in a same state or in a complemented state.

33. **(Previously Presented)** The method of claim 21, wherein the step of randomly selecting comprises a step of computing a parameter which is equal to a difference between the number of times when an operation of the second chain of operations is in the same state as in the first chain of operations and the number of times when an operation of the second chain of operations is in a complemented state with respect to the first chain of operations, and when the difference exceeds a given threshold, the step of randomly selecting a next operation of the second chain of operations in a normal state or in a complemented state is conducted so as to decrease this difference.

34 **(Previously Presented)** A method of performing an authentication cryptographic protocol between a server entity and a microcircuit entity in order to resist a DPA attack against the microcircuit entity during performing this authentication cryptographic protocol, comprising the steps of :

storing a DES comprising a first chain of operations in both the server entity and the microcircuit entity,

having a message exchanged between this server entity and this microcircuit entity,

having the server entity apply to the message the first chain of operations which is stored therein so as to obtain a server result,

having the microcircuit entity determine a second chain of operations from the first chain of operations which is stored in this microcircuit entity, this second chain of operations comprising a succession of operations each corresponding to a corresponding operation in the first chain of operations with each operation of the second chain of operations being the corresponding operation of the first chain of operations either in the same state or in the complemented state,

the step of having the microcircuit entity determine the second chain of operations from the first chain of operations comprising a step of randomly selecting, for at least a part of the second chain of operations corresponding to a corresponding part of the first chain of operations, either this at least a part of the operations of the first chain of operations in a same state as in the first chain of operations, or this at least a part of the first chain of operations in a complemented state,

the step of having the microcircuit entity determine the second chain of operations being such that at least some of the operations of this second chain of operations are in the same state as the corresponding operations in the first chain of operations whereas the other operations of this second chain of operations are in complemented state with respect to the corresponding operations of the first chain of operations,

having the microcircuit card apply this second chain of operations to the message so as to obtain a resultant message,

the step of having the microcircuit apply this second chain of operations comprising a step of selecting to output as the resultant message, depending on the step of having the microcircuit entity determine the second chain of operations, one of either the result of a last operation of the second chain of operations in a same state or the result of this last operation of the second chain of operation in a complemented state, and

comparing the resultant message obtained from the second chain of operations to the server result, and validating the authentication between the server entity and the microcircuit entity when the server result and the resultant message are identical.

35. **(Cancelled)**